UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/826,987	04/19/2004	Paul A. Gassoway	063170.7003	3477

5073 7590 03/02/2009

BAKER BOTTS L.L.P.
2001 ROSS AVENUE
SUITE 600
DALLAS, TX 75201-2980

EXAMINER	
ZEE, EDWARD	

ART UNIT	PAPER NUMBER
2435	

NOTIFICATION DATE	DELIVERY MODE
03/02/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ptomail1@bakerbotts.com
glenda.orrantia@bakerbotts.com

Office Action Summary	Application No.	Applicant(s)	
	10/826,987	GASSOWAY, PAUL A.	
	Examiner	Art Unit	
	EDWARD ZEE	2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 November 2008*.

2a)☒ This action is FINAL. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the amendments filed on November 21st, 2008. Claims 9, 27, 28 and 30 have been amended; Claims 1-34 are pending and have been considered below.

Claim Objections

2. Claims 9 and 28 remain objected to because of the following informalities: the term "operable to" is indefinite and should be amended to read "configured to" or the like. Appropriate correction is required.

The Applicant argues that the standing objection of the term "operable to" should be withdrawn, in light of the at least 120 patents issued by the Office on July 29th, 2008, which allegedly recited such a term within the patented set of claims. However, the Examiner respectfully submits that each and every patent application is individually considered by the Office and on a case by case basis. Thus, terms which may have been deemed proper by *another* Examiner regarding *another* set of claims, may or may not be pertinent to the terms recited in the instant set of claims.

Claim Rejections - 35 USC § 112

3. The amendments filed on November 21st, 2008 have been considered and are effective at overcoming the previous claim rejections, and thus have been withdrawn.

Claim Rejections - 35 USC § 101

4. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claims 9-15, 25, 28 and 31 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims 9-15, 25, 28 and 31 disclose a system, which in light of the specification [page 6, lines 21-22], appear to encompass a software application. Thus, Claims 9-15, 25, 28 and 31 are drawn to software per se. Software is not a series of steps or acts and this is not a process. Software is not a physical article or object and as such is not a machine or manufacture. Software is not a combination of substances and therefore not a compilation of matter. Thus, software by itself does not fall within any of the four categories of invention. Therefore, Claims 9-15, 25, 28 and 31 are not statutory.

The Examiner notes that as currently amended, the "reverse proxy server" now appears to be residing on "a processor controlled device". However, it may be unclear whether or not the system also comprises the "processor" or merely comprises the "reverse proxy server" residing on a "device" which is incidentally controlled by the processor.

Claim Rejections - 35 USC § 102

5. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

6. Claims 1-5, 9-11, 15-20, 24-32 and 34 are rejected under 35 U.S.C. 102(b) as being anticipated by Kindberg et al. (2003/0061515).

Claim 1: Kindberg et al. discloses a method for maintaining computer security comprising:

a. providing a signature file*(ie. a database containing capabilities, etc.)* containing information about known system vulnerabilities*(ie. acceptable arguments for a CGI script)* [page 4, paragraph 0054 & page 5, paragraphs 0058-0059];

b. at a reverse proxy server residing between at least one client computer and a web server [figure 2]:

i. receiving an incoming message from the at least one client computer, wherein the incoming message, if malicious and upon receipt by the web server, automatically causes the web server to perform an action which exploits a vulnerability of the web server*(ie. step 600)* [figure 6];

ii. comparing the received incoming message with the signature file to determine whether the incoming message is malicious*(ie. step 610)* [figure 6];

iii. and if it is determined to be malicious, blocking the incoming message from reaching the web server*(ie. request is rejected)* [page 4, paragraph 0054].

Claim 9: Kindberg et al. discloses a system for maintaining computer security comprising:

a. a signature file containing information about known system vulnerabilities, the information not including viral signature patterns [page 4, paragraph 0054 & page 5, paragraphs 0058-0059];

b. a web server [figure 2];

c. reverse proxy server residing on a processor controlled device between at least one client computer and a web server, the reverse proxy server operable to [figure 6]:

i. receiving an incoming message from the at least one client computer, wherein the incoming message, if malicious and upon receipt by the web server, automatically

causes the web server to perform an action which exploits a vulnerability of the web server [figure 6];

ii. comparing the received incoming message with the signature file to determine whether the incoming message is malicious [figure 6];

iii. and if it is determined to be malicious, blocking the incoming message from reaching the web server [page 4, paragraph 0054].

Claim 16: Kindberg et al. discloses a computer storage medium containing code for maintaining computer security comprising:

a. providing a signature file containing information about known system vulnerabilities, the information not including viral signature patterns [page 4, paragraph 0054 & page 5, paragraphs 0058-0059];

b. at a HTTP reverse proxy server residing between at least one client computer and a web server [figure 2]:

i. receiving an incoming message from the at least one client computer, wherein the incoming message, if malicious and upon receipt by the web server, automatically causes the web server to perform an action which exploits a vulnerability of the web server [figure 6];

ii. comparing the received incoming message with the signature file to determine whether the incoming message is malicious [figure 6];

iii. and if it is determined to be malicious, blocking the incoming message from reaching the web server [page 4, paragraph 0054].

Claim 34: Kindberg et al. discloses a method for maintaining computer security comprising:

a. providing a signature file containing information about known system vulnerabilities the information comprising a predefined length of a Universal Resource Locator ("URL") in a message header [page 4, paragraph 0054 & page 5, paragraphs 0058-0059];

b. receiving an incoming message from at least one client computer [figure 6];

c. comparing a length of a URL in a message header of the incoming message with the predefined length in the signature file to determine whether the incoming message is malicious*(ie. URL having a character string conforming to the length established)* [page 4, paragraph 0052];

d. and if the incoming message is determined to be malicious, blocking the incoming message from reaching a web server [page 4, paragraph 0054].

Claims 2-4, 10 and 17-19: Kindberg et al. discloses an invention as in claims 1, 9 and 16 above and further discloses that the comparing further comprises:

a. parsing the incoming message [page 4, paragraph 0055];

b. converting the incoming message into an internal format*(ie. specific CGI arguments etc.)* [page 5, paragraph 0060];

c. comparing the converted incoming message with the signature file and determining whether the converted incoming message is malicious based on the comparison*(ie. list of acceptable arguments etc)* [page 5, paragraph 0059];

d. reassembling the converted incoming message back into its original format prior to forwarding it to the web server if it is determined that the code is not malicious and forwarding the reassembled message to the web server*(ie. arugment passed through unchanged, etc.)* [page 5, paragraph 0061].

Claims 5, 11 and 20: Kindberg et al. discloses an invention as in claims 1, 9 and 16 above and further discloses that the signature file contains information about known system vulnerabilities*(ie. acceptable arguments for a CGI script)* [page 4, paragraph 0054 & page 5, paragraphs 0058-0059].

Claim 15: Kindberg et al. discloses a system as in claim 10 above and further discloses that the signature file is linked to the HTTP message analyzer module*(ie. list of acceptable arguments)* [page 5, paragraph 0058].

Claims 24-26: Kindberg et al. disclose a method, system and computer storage medium as in claims 1, 9 and 16 above, and further discloses that the incoming message comprises an HTTP messages [abstract].

Claims 27-29: Kindberg et al. discloses the invention of claims 1, 9 and 16, and further discloses that:

a. the information comprises a predefined length of a Universal Resource Locator ("URL") in a message header*(ie. URL having a character string conforming to the length established)* [page 4, paragraph 0052 & page 5, paragraphs 0058-0059];

b. and comparing the received incoming message with the signature file to determine whether the incoming message is malicious comprises determining whether the incoming message is malicious by comparing a length of a URL in a message header of the incoming message with the predefined length in the signature file [figure 6].

Claims 30-32: Kindberg et al. discloses the invention of claims 1, 9 and 16, and further discloses that the information comprises a list of known system vulnerabilities; and comparing the received incoming message with the signature file to determine whether the incoming

message is malicious comprises determining whether the incoming message is malicious by determining whether one or more characteristics of the incoming message satisfy one of the vulnerabilities on the list of known system vulnerabilities*(ie. character string length is not a bogus argument, etc.)* [page 5, paragraph 0058-0059].

Claim Rejections - 35 USC § 103

7. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

8. Claims 6-8, 12-14 and 21-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kindberg et al. (2003/0061515) in view of Cambridge (7,080,000).

Claims 6, 12 and 21: Kindberg et al. discloses a method, system and computer storage medium as in claims 1, 9 and 16 above, but does not explicitly disclose that the signature file is made available through a web server. However, Cambridge discloses a similar method, system and computer storage medium and further discloses that the signature file*(antivirus database)* is made available through a web server*(antivirus server)* [abstract]. Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to make the signature files available through a web server. One would have been motivated to do so in order to make signature file updates easily accessible.

Claims 7, 13 and 22: Kindberg et al. discloses a method, system and computer storage medium as in claims 1, 9 and 16 above, but does not explicitly disclose continuously updating the signature file. However, Cambridge discloses a similar method, system and computer storage medium and further discloses continuously updating the signature file*(antivirus data file)*

[column 2, lines 63-67]. Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to continuously update the signature file. One would have been motivated to do so in order to be able to detect the latest viruses, which are constantly being created.

Claims 8, 14 and 23: Kindberg et al. discloses a method, system and computer storage medium as in claims 1, 9 and 16 above, but does not explicitly disclose periodically downloading the signature file in order to make its copy current. However, Cambridge discloses a similar method, system and computer storage medium and further discloses periodically downloading the signature files*(receiving a new antivirus file at one of the user computers)* in order to make its copy current [abstract]. Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to periodically download the signature files. One would have been motivated to do so in order to be able to detect the latest viruses, which are constantly being created.

9. Claim 33 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kindberg et al. (2003/0061515) in view of El-Rafie (6,968,394).

Claim 33: Kindberg et al. discloses the method of claim 1, and further discloses logging user requests and in particular logging the user identity [page 4, paragraph 0056], but does not explicitly disclose that if the incoming message is determined to be malicious, identifying the first computer; and automatically blocking future messages received from the first client computer.

However, El-Rafie discloses a similar method and further discloses monitoring requests and identifying/blocking malicious users from future requests*(ie. determining rogue user terminals and blocking data flow to the offending IP address, etc.)* [column 26, lines 10-61].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to modify the method disclosed by Kindberg et al. with the features disclosed by El-Rafie in order to automatically provide a more selective access to resources within a network, as suggested by Kindberg et al. [page 1, paragraph 0012].

Response to Arguments

10. Applicant's arguments filed July 30th, 2008 have been fully considered but they are not persuasive.

11. Regarding Claims 1, 9 and 16: The Applicant argues that the Kindberg et al. reference does not disclose "comparing the received incoming message with the signature file to determine whether the incoming message is malicious; and if it is determined malicious, blocking the incoming message from reaching the web server", as recited in the instant claims. In particular, the Applicant suggests that Kindberg et al. fails to disclose determining if a message is malicious. However, the Examiner respectfully submits that Kindberg et al. appears to at least disclose excluding certain arguments that may subvert the behavior of the script in ways not intended by the script writer [page 5, paragraph 0058-0059]. Therefore, the Examiner respectfully disagrees and submits that the Kindberg et al. reference fairly suggests determining if a message is malicious by determining if the message contains malicious content*(ie. "bogus arguments" or the like).*

12. Regarding Claim 34: The Applicant argues that Kindberg et al. reference does not disclose "comparing a length of a URL in a message header of the incoming message with the predefined length in the signature file to determine whether the incoming message is malicious; and if the incoming message is determined to be malicious, blocking the incoming message from reaching web server. In particular, the Applicant suggests that Kindberg et al. fails to disclose comparing the received incoming message with the signature file to determine whether the incoming message is malicious. However, the Examiner respectfully disagrees for similar reasons as noted above in regards to Claims 1, 9 and 16.

Conclusion

13. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, THIS ACTION IS MADE FINAL. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to EDWARD ZEE whose telephone number is (571)270-1686. The examiner can normally be reached on Monday through Thursday 9:00AM-5:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

EZ
February 20, 2009
/Kimyen Vu/
Supervisory Patent Examiner, Art Unit 2435